

DPS:dsk

United States District Court  
STATE AND DISTRICT OF MINNESOTA

UNITED STATES OF AMERICA

CRIMINAL COMPLAINT

Case Number:

V.

SCOTT JAMES WHITCOMB

10-MJ-559-JSM

I, the undersigned complainant being duly sworn state the following is true and correct to the best of my knowledge and belief. On or about 8/4/2010, in Sherburne County, in the State and District of Minnesota, defendant(s)

did knowingly distribute visual depictions that had been mailed, shipped and transported in interstate commerce, by computer, where the production of such visual depictions involved the use of a minor engaged in sexually explicit conduct and such depictions are of such conduct, including, but not limited to, the following computer image files: P101-Webcam-12Yo Boy Get Sucked-Bibcam-Webcamboy-Fxg Older Brother Sucks off His Preteen Bro Till He Orgasums And His Whole Body Jerks- Gay Pedo Pthc.avi, all in violation of Title 18, United States Code, Sections 2252(a)(2) and 2252(b)(1).

in violation of Title 18, United States Code, Section(s) 2252(a)(2) and 2252(b)(1).

I further state that I am a(n) Special Agent and that this complaint is based on the following facts:

SEE ATTACHED AFFIDAVIT

Continued on the attached sheet and made a part hereof: ☒ Yes ☐ No

Sworn to before me, and subscribed in my presence,

12/21/10  
Date

The Honorable Janie S. Mayeron  
UNITED STATES MAGISTRATE JUDGE

Name & Title of Judicial Officer

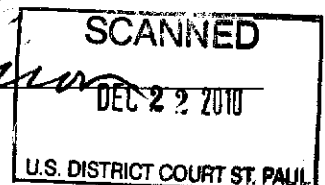
*Robert Blackmore*

Signature of Complainant  
Robert Blackmore  
FBI

St. Paul, MN

City and State

*Janie S. Mayeron*  
Signature of Judicial Officer



**THE FOLLOWING IS FURNISHED FOR INFORMATION ONLY:**

DEFENDANT'S NAME: \_\_\_\_\_

ALIAS: \_\_\_\_\_

LAST KNOWN RESIDENCE: \_\_\_\_\_

LAST KNOWN EMPLOYMENT: \_\_\_\_\_

PLACE OF BIRTH: \_\_\_\_\_

DATE OF BIRTH: \_\_\_\_\_

SOCIAL SECURITY NUMBER: \_\_\_\_\_

HEIGHT: \_\_\_\_\_ WEIGHT: \_\_\_\_\_

SEX: \_\_\_\_\_ RACE: \_\_\_\_\_

HAIR: \_\_\_\_\_ EYES: \_\_\_\_\_

SCARS, TATTOOS, OTHER DISTINGUISHING MARKS: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

FBI NUMBER: \_\_\_\_\_

COMPLETE DESCRIPTION OF AUTO: \_\_\_\_\_

\_\_\_\_\_

INVESTIGATIVE AGENCY AND ADDRESS: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

**AFFIDAVIT IN SUPPORT OF**  
**A CRIMINAL COMPLAINT**

**AFFIDAVIT OF SPECIAL AGENT ROBERT J. E. BLACKMORE**

I, Robert J. E. Blackmore, being duly sworn, hereby depose and say:

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been so employed for over 10-years. I am currently assigned to the Minneapolis, Minnesota, Division of the FBI and work on the Minnesota Cyber Crime Task Force. I have received specialized FBI training in both the investigation of computer and computer-related crimes and crimes involving the sexual exploitation of children. As a member of the Cyber Crime Task Force, my responsibilities include the investigation of various criminal offenses involving computers, computer networks, and the Internet, including the investigation of crimes involving the sexual exploitation of children. While employed by the FBI, I have participated in numerous investigations in which I have collected evidence in an electronic form.

2. This affidavit is submitted in support of an application for a criminal complaint and arrest warrant charging Scott Whitcomb (hereafter, "Whitcomb"), 48 years of age, and residing at a residence in, Zimmerman, Minnesota, with violations of Title 18 U.S.C. §§ 2251 and 2252.

3. The statements in this affidavit are based in part on information provided by other law enforcement officers, and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a criminal complaint and arrest warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause for the issuance of a criminal complaint charging Whitcomb with the production, distribution, and possession, of child pornography in violation of Title 18 U.S.C. §§ 2251 and 2252.

**STATUTORY AUTHORITY**

4. This investigation concerns alleged violations of Title 18 U.S.C. §§ 2251 and 2252, relating to material involving the sexual exploitation of minors.

a. 18 U.S.C. § 2251(a) prohibits the use, persuasion, inducing, enticing, or coercing of a minor to in interstate or foreign commerce with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.

b. 18 U.S.C. § 2252(a)(2) prohibits knowingly receiving or distributing in interstate or foreign commerce, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct.

c. 18 U.S.C. § 2252(a)(4) prohibits possessing one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been transported in

interstate or foreign commerce, or that were produced using materials that had traveled in interstate or foreign commerce.

**DEFINITIONS**

5. The following definitions apply to this Affidavit and Attachment B:

- a. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.
- b. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).
- c. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* 18 U.S.C. § 1030(e)(1).
- d. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit

electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

e. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to

configure or use computer hardware, computer software, or other related items.

g. “Computer software” is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

i. “Minor” means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

j. “Peer-to-peer file-sharing” (P2P) is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. A user obtains files by

opening the P2P software on the user's computer, and conducting searches for files that are currently being shared on another user's computer.

k. "Sexually explicit conduct" applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

l. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

m. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs),



memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

#### **BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY**

6. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

7. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

8. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

9. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

10. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

11. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

12. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

13. A growing phenomenon on the Internet is peer-to-peer file-sharing (P2P).

14. The latest evolution of P2P software is a program that allows a user to set up his own private P2P network of contacts. File-sharing through this new and publicly available P2P file-sharing program is limited only to other users who have been added to a private list of

“friends.” A new user is added to a list of friends by request. Acceptance of a friend request will allow that new user to download files from the user who sent the friend request. The new user can then browse the list of files that the other user has made available to download, select desired files from this list, and download the selected files. The downloading of a file occurs through a direct connection between the computer requesting the file and the computer containing the file.

15. One aspect of P2P file sharing is that multiple files may be downloaded in parallel, which permits downloading more than one file at a time.

16. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four sets of numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

17. Third-party software is available to identify the IP address of the P2P computer sending the file. Such software monitors and logs Internet and local network traffic.

### **BACKGROUND OF THE INVESTIGATION**

18. On August 4, 2010, an officer with the Minneapolis Police Department, who is assigned the Minnesota Internet Crimes Against Children Task Force, and conducts online undercover operations was searching a publically available P2P file sharing network for images and videos of child pornography that were being offered for distribution by other users of the network. The software program used by the officer is only available to law enforcement.

19. During this online search the officer received information that one or more files of child pornography were available for download from IP address 208.38.111.99. The officer browsed IP address 208.38.111.99 and received a file list from the host computer. The list

received by the officer contained eight (8) files, of which five (5) matched suspected child pornography Secure Hash Algorithm (SHA1) values contained in the peer to peer database.

20. SHA1 is like a fingerprint, or DNA, of a digital file. This allows an investigator to see files being traded on a P2P system that are previously known to depict child pornography and know that they are the same based on the SHA1 value.

21. The officer was able to make a direct connection to computer using IP address 208.38.111.99 and download the following file completely from this one (1) IP address:

- a. P101-Webcam-12Yo Boy Get Sucked-Bibcam-Webcamboy-Fxg Older Brother Sucks Off His Preteen Bro Till He Orgasums And His Whole Body Jerks- Gay Pedo Pthc.avi

-This file is approximately 2 minutes 47 seconds long and depicts a nude boy wearing only white socks. There is an adult male performing oral sex on the boy who appears to be between 10-12 years old.

22. Based on his training and experience, the officer knew this video file to be child pornography.

23. In addition to the file he downloaded, the officer was able to determine by the SHA1 values he observed that at least two (2) other video files being offered by the computer using IP address 208.38.111.99.

24. The officer used open source information to determine that IP address 208.38.111.99 is registered to Iowa Telecom.

25. In response to an administrative subpoena, Iowa Telecom advised that the subscriber for this IP address was Scott Whitcomb, with an address in Zimmerman, Minnesota.

26. The information contained in paragraphs 18 – 25 was provided to the Sherburne County Sheriff's Office where it was reviewed by an investigator. Based on this information, an investigator obtained a State of Minnesota search warrant from the Sherburne County Court which authorized the search of Scott Whitcomb's, Zimmerman, Minnesota address. The signed search warrant allowed the officers to enter the residence and search for all forms of media containing pornographic works involving children.

27. On December 16, 2010, officers from the Sherburne County Sheriff's Office served the aforementioned search warrant at the residence of Scott Whitcomb. When this search warrant was served the residence was unoccupied.

28. Among the items located and subsequently seized pursuant to the warrant were a desktop computer that was located in the living room area of the residence and a laptop computer that was located in what appeared to be the master bedroom.

29. The laptop computer was given to a Sherburne County Forensics Investigator who performed a forensic preview of the laptop. During the forensic preview the Forensics Investigator discovered what she believed to be images of child pornography under "Scott's Profile".

30. An investigator reviewed these images and observed them to depict a fully naked boy believed to be between 12 – 14 years old whose genitalia was fully exposed in all the images. In two of the images the boy is touching his genitalia.

31. Further inspection of these images showed that the background and bedding in the images was consistent with that from within that residence. The photos also showed the bed in its current location and the same double pane window and shades. An alarm clock, nightstand, and remote control depicted in the images were discovered during the search. Based on these

observations, it was believed that the pornographic images of the juvenile boy in the residence specified in the search warrant.

32. An investigator made contact with Whitcomb in Minneapolis, Minnesota. The investigator informed Whitcomb that he wished to take a voluntary taped statement regarding an ongoing criminal investigation. Whitcomb agreed to be interviewed. Whitcomb stated that he was the sole occupant of the residence in Zimmerman, Minnesota. The investigator then informed Whitcomb that a search warrant had been executed at his residence and that the search was executed for images containing child pornography. At that point Whitcomb requested that the taped statement be terminated. The investigator discontinued the interview.

33. Investigators determined that a juvenile boy depicted in the pornographic images on a laptop from Whitcomb's residence was positively identified as L.R.O., date of birth in 1995. Contact was made with L.R.O.'s father who agreed to transport his son to the Sheriff's Office to be interviewed.

34. Based on the positive identification of the juvenile boy depicted in the images found on the laptop from Whitcomb's residence, the investigator then placed Whitcomb under arrest for probable cause for possession of pornographic works involving a minor, MN Statute 617.247.

35. After transporting Whitcomb to the Sherburne County Jail the investigator received further information that the victim L.R.O. had a younger brother, D.M.O., date of birth in 1998. Preliminary information indicated that both boys had been victims of multiple acts of criminal sexual conduct over a two (2) to three (3) year period, that included both sexual contact and penetration.

36. In a statement to an investigator, L.R.O. stated that approximately six (6) years ago, Whitcomb had a juvenile at his residence identified as P.M.E., date of birth in 1995. L.R.O. and P.M.E. became friends during this time and would spend time at Whitcomb's residence. L.R.O. stated that initially there was nothing sexual in nature. However, in the past two (2) to three (3) years there had been multiple acts of criminal sexual conduct. L.R.O. stated that those sexual acts were performed on himself, his younger brother, and P.M. E. and that often times photographs and films of the sexual acts were produced.

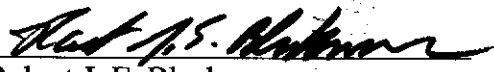
37. L.R.O. stated that on at least two occasions he was asked to perform oral sex on Whitcomb. L.R.O. stated that on both occasions he began the act of performing oral sex but stopped after a short period of time. L.R.O. further advised that on at least 10-15 occasions, Whitcomb had performed oral sex on L.R.O. L.R.O. stated that on at least 25 other occasions Whitcomb would place his hands inside his pants and masturbate him.

38. L.R.O. stated that he and the other victims were asked to or forced to watch adult pornography. The victims were also asked to masturbate so that Whitcomb could watch the boys complete these acts. Whitcomb rewarded the boys with gifts such as Xbox games and other items.

39. A statement was obtained from D.M.O. by investigators. The investigators advised that D.M.O.'s statement was very consistent in the sexual acts that the boys were subject to, including the coercing or forcing of the boys to further extents than described by L.R.O.

Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe Scott Whitcomb knowingly possessed and distributed child pornography in violation of Title 18, U.S.C. §§ 2251 and 2252.

40. Your affiant, therefore, respectfully requests that a criminal complaint and arrest warrant be issued for Scott Whitcomb.

  
Robert J. E. Blackmore  
Special Agent  
Federal Bureau of Investigation

Sworn and subscribed before me this 21<sup>th</sup> day of December, 2010.

  
Jamie S. Mayeron  
UNITED STATES MAGISTRATE JUDGE